*2018 International Conference on Computing, Power and Communication Technologies (GUCON)*
*Galgotias University, Greater Noida, UP, India. Sep 28-29, 2018*

# Data Access Security in Cloud Computing: A Review

Anagha Markandey
*Information Technology*
MITSOE Pune, India
ana.markandey@gmail.com

Prajakta Dhamdhere
*Information Technology*
MITSOE Pune, India
prajaktab064@gmail.com

Yogesh Gajmal
*Information Technology*
MITSOE Pune, India
yogeshmgajmal@gmail.com

***Abstract*— Now a days, the big data is stored on the internet called as clouds. With usage of cloud storage users can store their data on the internet. Cloud computing provides various services to the users. Data storage is one of them. But it is observed that there is very big problem of data stealing through the internet. More is the problem of data leaking & attacks on the data on clouds. The intention of this paper is to attain data security of cloud storage and to put together equivalent cloud storage security strategy. These strategies are combined with the outcomes of existing data by considering the security risks & user data on cloud storage & move towards the appropriate security technique , which is based on properties of cloud storage system. The paper will go in to subtle elements of information assurance strategies and methodologies utilized all through the world to guarantee most extreme information insurance by diminishing dangers and dangers. Accessibility of information in the cloud is helpful for some applications yet it postures hazards by presenting information to applications which may as of now have security provisos in them. Also, utilization of virtualization for distributed computing may chance information when a visitor OS is keep running over a hypervisor without knowing the unwavering quality of the visitor OS which may have a security proviso in it. The paper will likewise give a knowledge on information security perspectives for Data-in-Transit and Data-at-Rest.**

***Keywords—Cloud Computing, Cloud Storage, Data Security, Cloud Services.***

## I. INTRODUCTION

Basically the concept of cloud computing is invented due to the need of various services like networking , security, storage, and artificial intelligence as well as standard office applications. So, cloud computing can be defined as the program outsourcing. Using cloud, one can use various applications & software from anywhere in the world, which are provided by some third party called as cloud. There are various benefits of cloud computing such as,

- Self-service provisioning in which the users can use the various compute resources for any kind of work demand.
- Elasticity, in which one can increase the data usage as demand increases & decrease the data usage as demand decreases. This reduces the massive investment.
- Workload flexibility, in which Cloud service providers frequently implement outmoded resources to ensure flexible storage and it keep users' vital workloads working across many global regions.
- Migration flexibility, in which the users can transfer the data from one cloud to another cloud as per requirement.

Cloud is categorised into 3 types,

1. Infrastructure as a service (IaaS) in which the cloud hosts essentials of infrastructure like servers, software, storage, etc. Also provides the data security, maintenance, data backup, etc.
2. Software as a service (SaaS) in which various applications are able to use.
3. Platform as a service (PaaS) in which the users can develop their own application, run it and manage those applications on cloud without getting stuck into code, infrastructure & storage.

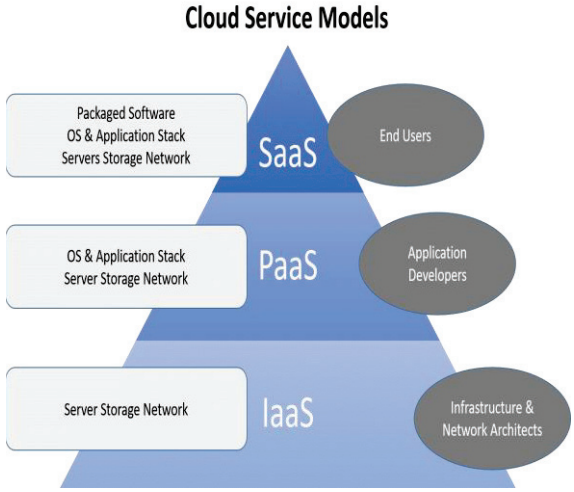


Fig. 1. Cloud Computing Types

Generally, cloud provides the services as networking, security, storage, artificial intelligence, etc. So, to avail those services, various organizations rent to the cloud service providers. Now, here is the responsibility of the vendor to provide the services to the customers as per their requirement. But, every coin has two sides, i.e. there are some problems with this super technology such as data security. Means, when the confidential data is uploaded on the cloud, it may be hacked by some third party, so the main issue is of the big data security stored on the cloud now a days.

### *A. Cloud Storage*

Distributed storage is innovation that enables you to spare documents away, and afterward get to those records by means of the Cloud. We should separate this definition. To begin with, capacity is the PC's capacity to spare documents

and different assets for later utilize. When you restart a PC, the documents that are as yet accessible after the PC walks out on are spared and perused from capacity. Such capacity usually comprises of a hard drive, a USB Flash drive, or another kind of drive.

Since neighbourhood information drives can be harmed or stolen, a thought was produced to utilize information drives over a system as capacity. This enables the drives to be secured in a server farm and moved down naturally. At first, organize capacity required quick neighbourhood systems (LAN), however today we have a universal system called the Internet.

The second piece of Cloud Storage, the Cloud, speaks to the Internet. Any administration, including capacity, accessible over the Internet, is called Cloud benefit. On the off chance that you utilize GMAIL it is email in the Cloud, on the off chance that you utilize an Amazon MP3 player, that is music in the Cloud.

- Google Docs enables clients to transfer reports, spreadsheets and introductions to Google's information servers. Clients can alter records utilizing a Google application. Clients can likewise distribute archives so other individuals can read them or even make alters, which implies Google Docs is additionally a case of distributed computing.
- Web email suppliers like Gmail, Hotmail and Yahoo! Mail store email messages without anyone else servers. Clients can get to their email from PCs and different gadgets associated with the Internet.
- Locales like Flickr and Picasa have a huge number of computerized photos. Their clients make online photograph collections by transferring pictures specifically to the administrations' servers.
- YouTube has a huge number of client transferred video records.
- Site facilitating organizations like StartLogic, Hostmonster and GoDaddy store the records and information for customer Web locales.

*B. Need of Cloud Storage Security*

Distributed storage security is currently massively prevalent. A current review demonstrated that 95% of IT experts are utilizing distributed storage.

That number is required to keep on growing quickly. It's evaluated that 2.3 billion individuals will utilize distributed storage by 2020.

*C. Advantages of Cloud Storage Security*

1. Information Encryption : Information you store on a cloud can be scrambled either previously or after you send it, giving included insurance.

There is a scope of distributed storage security alternatives, including Single Sign-On (SSO), Multi-Factor Authentication (MFA) and that's just the beginning. This implies your information must be gotten to by the general population you need it to, regardless of whether your gadget is stolen. Your security is totally ensured and you don't have to stress over your information being stolen or sold off.

2. It Pays to Have a Back-Up :Putting away every one of your information on one server is extremely unsafe. On the off chance that it comes up short for any reason, you could lose everything in a moment. Regardless of whether you don't utilize distributed storage as your essential stockpiling framework, it can work as a place to store second duplicates of documents in the event that you ever require a move down. In case you're as of now utilizing distributed storage, you don't need to stress over support anything up yourself. The framework removes the problem from that by doing it for you.

3. Ensure Against Hackers: Putting away your information on a cloud framework gives included assurance from programmers and information misfortune. It's not simply private ventures that are defenseless against programmers. At the point when bigger organizations get hacked, it generally drums up a buzz in the media. Understood organizations which have succumbed to popular hacking embarrassments incorporate Sony, LinkedIn, Target and Ashley Madison. Every one of these organizations' notorieties endured a shot thus. Try not to give your business a chance to endure a similar destiny. As indicated by Duke University, 80% of all US organizations have experienced some sort of hacking, so neglecting to shield yourself from the likelihood is to a great degree unsafe. In any case, hacking isn't your lone concern. Your organization could likewise endure information misfortune because of a server disappointment or human mistake. Mists are went down to different servers, so you never need to stress over losing the data you keep on them. On the off chance that one server crashes, your information will at present be securely put away in different areas. This altogether diminishes the danger of information misfortune. Equipment disappointment and specialized glitches are totally capricious, and there's no motivation to abandon yourself powerless against them when there's distributed storage accessible. Putting away your information on a cloud framework gives included assurance from programmers and information misfortune.

## II. LITRATURE SURVEY

Cloud registering condition relies upon client administrations, for example, fast stockpiling and recovery gave by distributed computing framework. Meanwhile' information security is an imperative issue to comprehend critically for distributed storage innovation. Lately, There are an ever increasing number of vindictive assaults on distributed storage frameworks, and distributed storage arrangement of information spilling additionally every now and again happened. Distributed storage security concerns the client's information security. The motivation behind this paper is to accomplish information security of distributed storage and to figure relating distributed storage security strategy. Those were joined with the consequences of existing. Scholarly research by examining the security dangers of client information in distributed storage and approach a subject of the significant security innovation, which in light of the auxiliary attributes of cloud capacity framework[1].

In this paper, they attempted to propose the security blemish of their plot when dynamic enemies are associated with distributed storage. A dynamic foe is equipped for

altering the information put away in cloud subjectively. This information adjustment isn't being recognized by the client and the examiner in the check procedure. They attempted to propose an answer for resolve this defect by marking the confirmation reaction produced on the cloud server side. At that point the marked verification is sent to the put stock in outsider examiner (TTPA) for confirmation. The examiner initially confirms the mark and for the approval of the verification. The proposed conspire is ended up being secure against dynamic enemy[2].

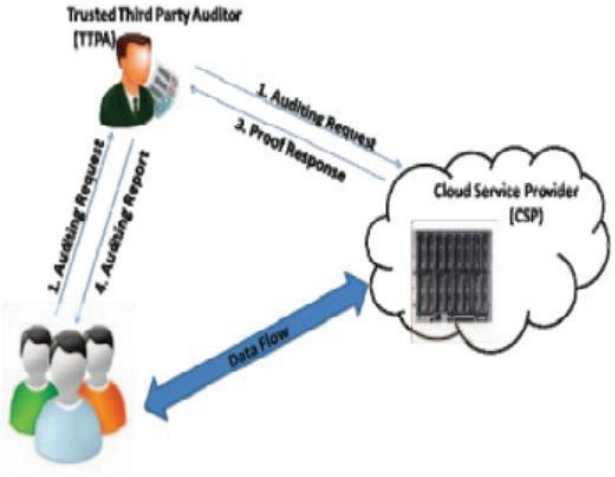


Fig. 2. System Model

Venture frameworks give coordinated data to all exercises in an association. These frameworks fill in as a key resource for any association and thus it ends up compulsory to guarantee their security. Data security joins frameworks, activities and inward controls to guarantee the accessibility, honesty and privacy of information and operational methodology in an association. In the present situation these administrations are offered on the cloud chiefly to diminish inalienable hazard related with the conventional endeavour frameworks. Distributed computing speaks to a huge move in the way that IT assets are overseen, worked, and devoured. This change opens a few advantages to undertakings, advancing more prominent IT effectiveness and nimbleness. This paper is proposed to recommend a security structure of big business frameworks on cloud[3]. The author proposed security framework for cloud based enterprise system is given above,

To fathom the information security in distributed computing, author have proposed another structure in view of Hybrid Encryption Plans which can scramble and recover the information effectively. The execution assessment and approval of the proposed show is done and the after effect of execution examination b demonstrated that our engineering are practical, adaptable and effective [4].

In this paper authors presented a model for provable the information ownership (PDP) that permits a customer that has put away information at an untrusted server to confirm that the server has the first information without recovering it. The model creates probabilistic verifications of ownership by inspecting arbitrary arrangements of squares from the server, which definitely decreases I/O costs. The customer keeps up a steady measure of metadata to confirm the evidence. The challenge/reaction convention transmits a little, steady measure of information, which limits organize

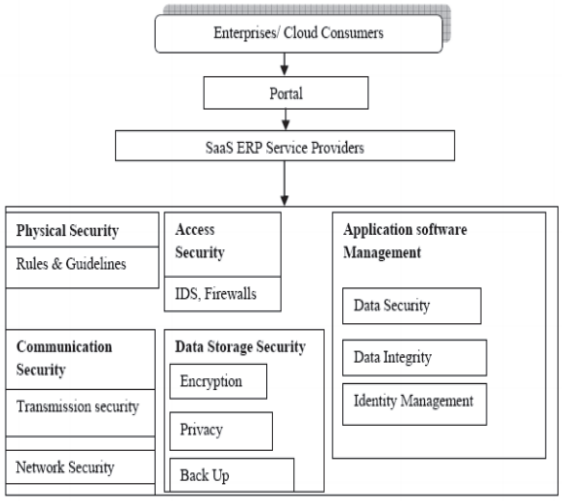


Fig. 3. security framework for cloud based enterprise system

correspondence. Accordingly, the PDP show for remote information checking underpins vast informational collections in generally dispersed capacity frameworks. It is likewise predominant in execution by limiting the utilization of costly open enter cryptography in metadata administration. They introduced the design and execution of different SHAROES parts and our tests show execution better than different proposition by finished 40% on various benchmarks[5].

## III. FUTURE SCOPE

Distributed computing security challenges are a piece of continuous research. Different open issues are distinguished as future extension.

### *A. Data Classification in view of Security*

A distributed computing server farm can store information from different clients. To give the level of security in view of the significance of information, characterization of information should be possible. This characterization plan ought to think about different angles like access recurrence, refresh recurrence and access by different elements and so on based on the sort of information. Once the information is ordered and labelled, at that point level of security related with this particular labelled information component can be connected. Level of security incorporates classification, encryption, respectability and capacity and so on that are chosen in view of the kind of information.

### *B. Character administration framework:*

Cloud registering clients are distinguished and utilized their characters for getting to the administrations. A protected trust based personality administration conspire is basically a need by all cloud specialist organization and clients. Different issues of personality administration framework are recognized. Answer for secure id-age and appropriation, capacity and life cycle administration is an interest for trust based personality administration framework.

### *C. Secure put stock in based Solution for distributed computing Service:*

A safe domain for execution of the distributed computing administrations alongside general security contemplations is a challenge. A protected and trusted arrangement is the

prerequisite that should be engaged and tended to by the distributed computing foundation.

## IV. CONCLUSION

Cloud computing is a promising and rising innovation for the up and coming age of IT applications. The hindrance and obstacles toward the quick development of cloud computing are data security and protection issues. Decreasing data stockpiling and preparing cost is a compulsory prerequisite of any association, while examination of information and data is dependably the most essential undertakings in every one of the associations for basic leadership. A writing survey of the works in the zone of cloud computing data security is directed and the perceptions of audit are introduced in this paper.

## REFERENCES


[1] DIAO Zhe, WANG Qinghong, SU Naizheng, ZHANG Yuhan, "Study on Data Security Policy Based On Cloud Storage", 2017 IEEE 3rd International Conference on Big Data Security on Cloud.

[2] T. Subha, Dr. S. Jayashri, "Efficient Privacy Preserving Integrity Checking Model for Cloud Data Storage Security", 2016 IEEE Eighth International Conference on Advanced Computing (ICoAC)

[3] Binu, M. S., & Meenakumari, J. (2012). "A security framework for an enterprise system on cloud." Indian Journal of Computer Science and Engineering (IJCSE), 3(4), 548-552.

[4] "Ensuring data storage security in cloud computing based on hybrid encryption schemes", Mrinal Sarkar, Sanjay Kumar, 2016 fourth international conference on parallel, distributed & grid computing.

[5] "Data Security in Cloud computing and Outsourced Databases", ShankarNayak Bhukya, Dr.Suresh Pabboju, Dr. K Venkatesh Sharma, International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[6] Feng Deng-Guo,Zhang Min,Zhang Yan.Study on cloud computing security.Journal of Software,2011,22(1):71-83(in Chinese)

[7] Bai Xin .Research on Key Technology of Safety Monitoring Mechanism in Cloud Environment[D].Beijing industry university.2015(in Chinese)

[8] Hai JiaJia.Research on User Data Storage Security in Cloud Environment[D].Heilongjiang University.2015(in Chinese)

[9] Feng Chao-Sheng,Qin Zhi-Guang,Yuan Ding.Cloud data secure storage technology[J].Journal of Computer Science,2015,(01):150-163.(in Chinese)

[10] Q.Wang,C.Wang,J.Li,K.Ren,W.Lou.Enabling public verifiability and data dynamics forstorage security in cloud computing [C]// 14th European Symposium on Research in Computer Security,Springer Berlin/Heidelberg,2009:355-370

[11] Wenhong Tian, Yong Zhao.An Introduction to Cloud Computing[J].Cloud Resource Management and Scheduling,2015:1-15.

[12] Deyan Chen,Hong Zhao.Data Security and Privacy Protection Issues in Cloud Computing[C].2012 International Conference on Computer Science and Electronics Engineering(ICCSEE),PP.647-651

[13] Wang C,Wang Q,Pen K,etal.Privacy-preserving public auditing for data storage security in cloud computing[C].In Proceeding s of IEEE INFO.COM'10,2010:14-19